IPCop – Open Source Firewall/VPN/IDS
Part One – Simple How-To

Joseph Guarino
Evolutionary IT
www.evolutionaryit.com

What is IPCop

The IPCop project is a GNU/GPL open source project that offers an exceptional feature packed stand alone firewall to the internet community. Its comprehensive web interface, well documented administration guides, and its involved and helpful user/administrative mailing lists make users of any technical capacity feel at home. It goes far beyond a simple ipchains / netfilter implementation available in most Linux distributions and even the firewall feature sets of commercial competitors.

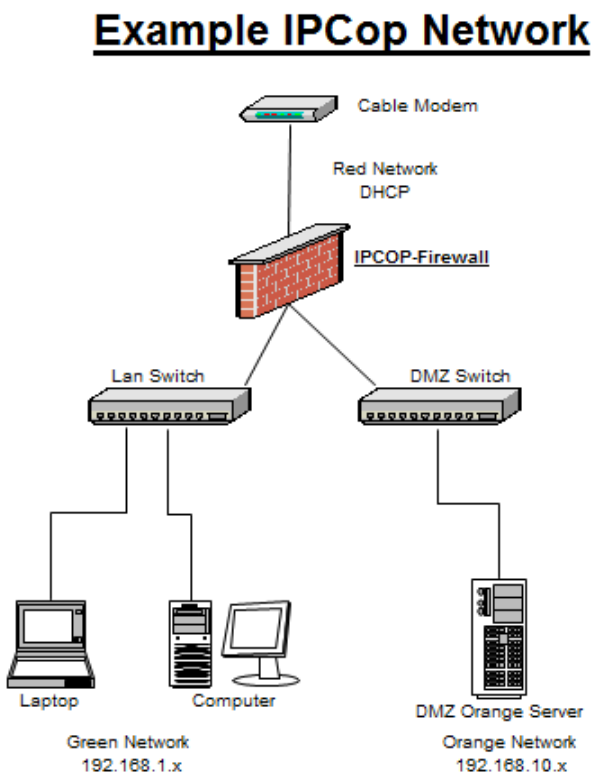
Firewalls have had to undergo a tremendous metamorphosis as a result of evolving threats. IPCop is exemplary in offering such a range of default features and even further a large set of optional plug-ins which can provide further functionality.

Some of IPCops impressive base install features include: secure https web administration GUI, DHCP Server, Proxying (Squid), DNS Proxying, Dynamic DNS, Time Server, Traffic Shaping, Traffic/Systems/Firewall/IDS graphing, Intrusion Detection (Snort), ISDN/ADSL device support and VPN (IPSec/PPTP) functionality. As if these base features were not an astounding enough there are dozens of add-ons which can further expand the functionality of your IPCop from Web Filtering to Anti virus scanning.

Pre-Requisites for Your IPCop

IPCop installation generally runs 25 minutes, and you can complete it with relatively modest hardware requirements such as a 386 processor with 32MB RAM and >300MB of disk, and 3 Network Cards (2 if there is no need for a DMZ). If you plan to utilize caching proxy, IDS or other add-ons, consider additional horsepower in terms of RAM/Processor.

Building Your IPCop
386 Processor with 32MB RAM, 300MB hard disk and 3 Network Cards
2 x 5 port 10/100/1000 switch
Network Cables



Architectural Decisions: Segmentation

One essential consideration you have to make before installing is network architecture (segmentation/address space). IPCop uses color-coding system of Red, Green, Blue and Orange to describe the "roles" or security levels which an interface/network segment will have in protecting your network. Color coding is logical in that it represents a continuum of network access from restricted to permissive. A RED interface is your untrusted interface/segment like the Internet, whereas Green is the "trusted" interface/segment of your internal network. Additionally, Blue is for a separate segment for Wireless Devices, while Orange is for a DMZ or where any publicly accessible servers you want available to the Internet. In this case we are only configuring a Green/Red/Orange network installation with 3 network interfaces one of which is your cable broadband providers cable modem (Ethernet).

Understanding and Picking your address space

Before you begin it is important to know how your ISP TCP/IP settings. Does your ISP give you a DHCP address or a static IP address? In many cases simply going to your ISP's "Support" page offers you this information. Most ISPs use DHCP to dynamically allocate IP address space so you get a non-static IP address that applies to your RED interface. Make note of the TCP/IP setting your ISP would have you use before you install.

In architecting your IPCop solution you have the choice of setting up NAT (Network Address Translation) network address space. Green, Blue and Orange networks depend entirely on how

many nodes or machines you will have on each network. There are 3 network spaces defined by the standards body, IETF, that can be used for these NAT'ed networks and they are:

10.0.0.0	-	10.255.255.255 (10/8 prefix)
172.16.0.0	-	172.31.255.255 (172.16/12 prefix)
192.168.0.0	-	192.168.255.255 (192.168/16 prefix)

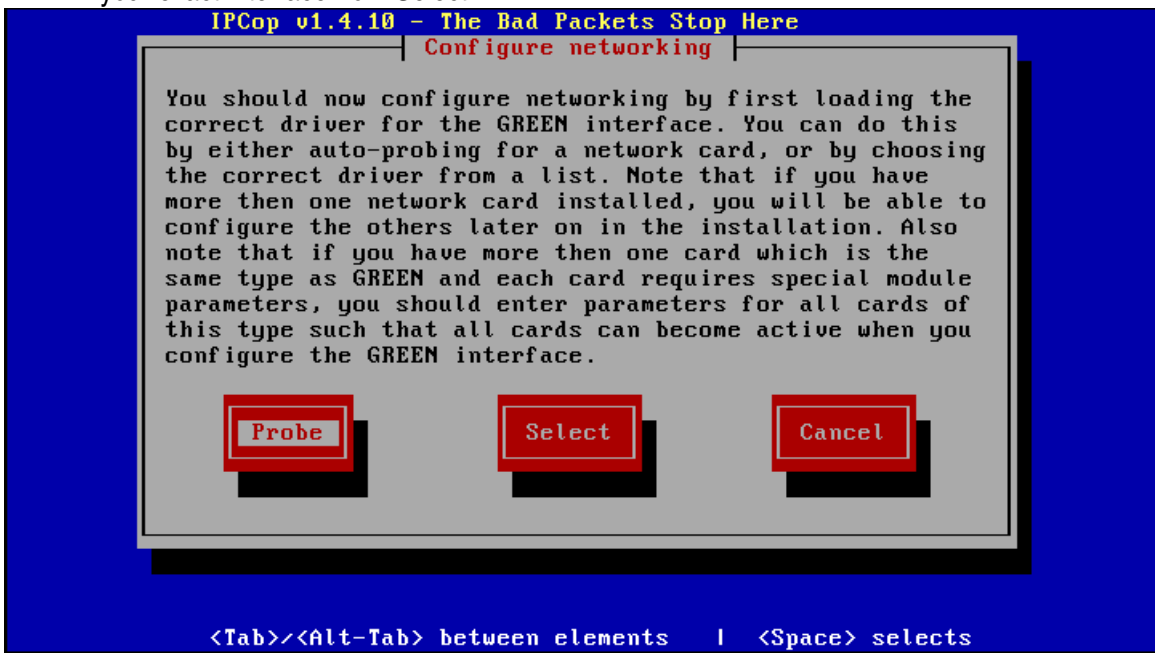
If your Green network contains 15 hosts you can use 192.168.1.2-16. Your Green interface will run DHCP and pass out addresses to your internal network in this range. The same logic applies to address space on your Orange or "DMZ" network select a network space appropriate for the number of hosts/networks you will require.

Installing your IPCop

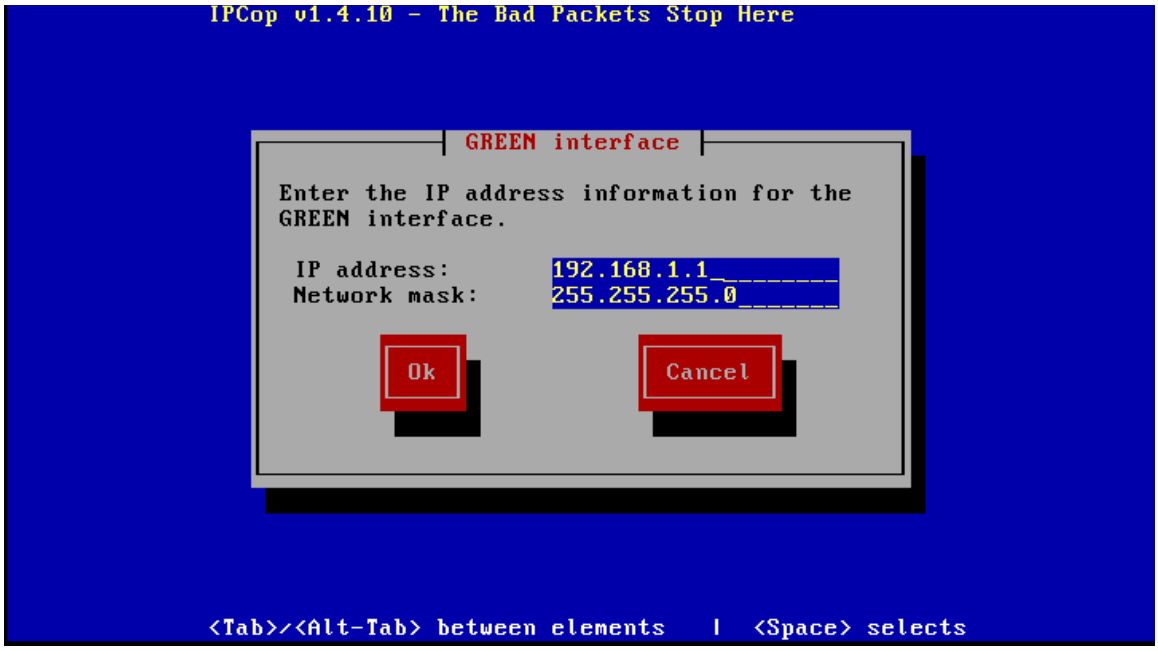
Verify hardware compatibility at IPCop website.
Download the ISO's and burn them.
Connect all the physical layer i.e. Ethernet cables, hook up your monitor, keyboard and mouse to the machine that will be your IPCop
Boot off the CD.
Run through the simple prompt-based installation. NOTE: These are all very self-explanatory steps such as selecting your Language. The arrow Keys, Tab and Enter will help you navigate.

Install Process

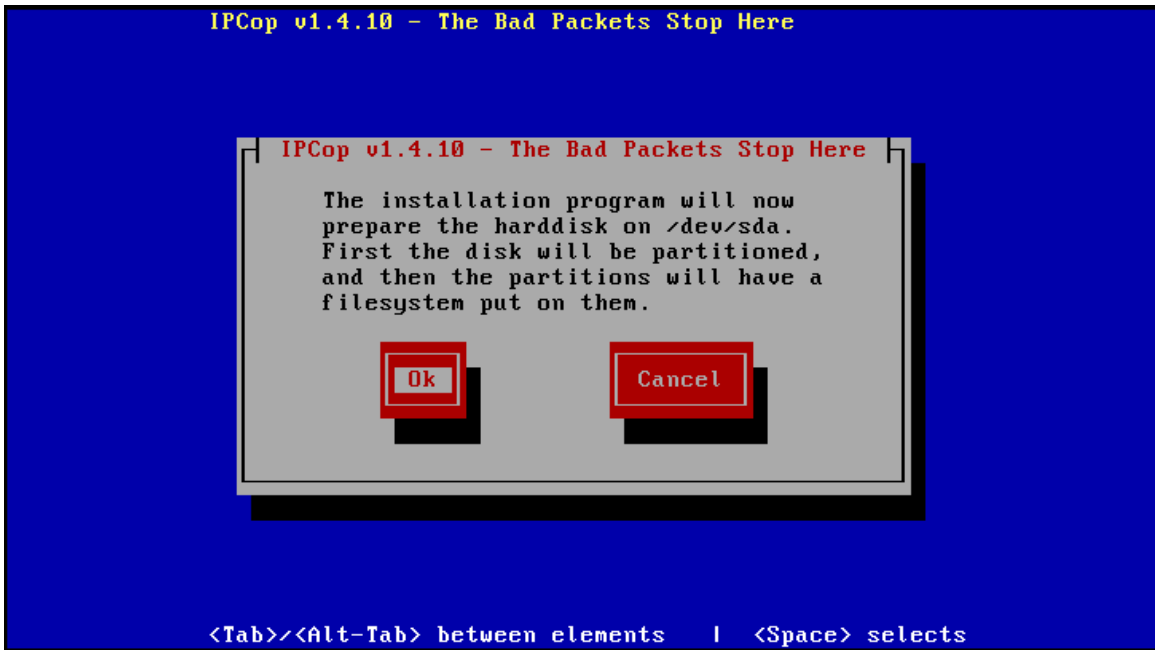
- Select your language.
- Select your "Installation Medium", a CD in this case.
- Configure your network cards – The fastest way to configure your network interface cards is by selecting "Probe" option. If you know the network card information you can choose to your exact interface from Select.



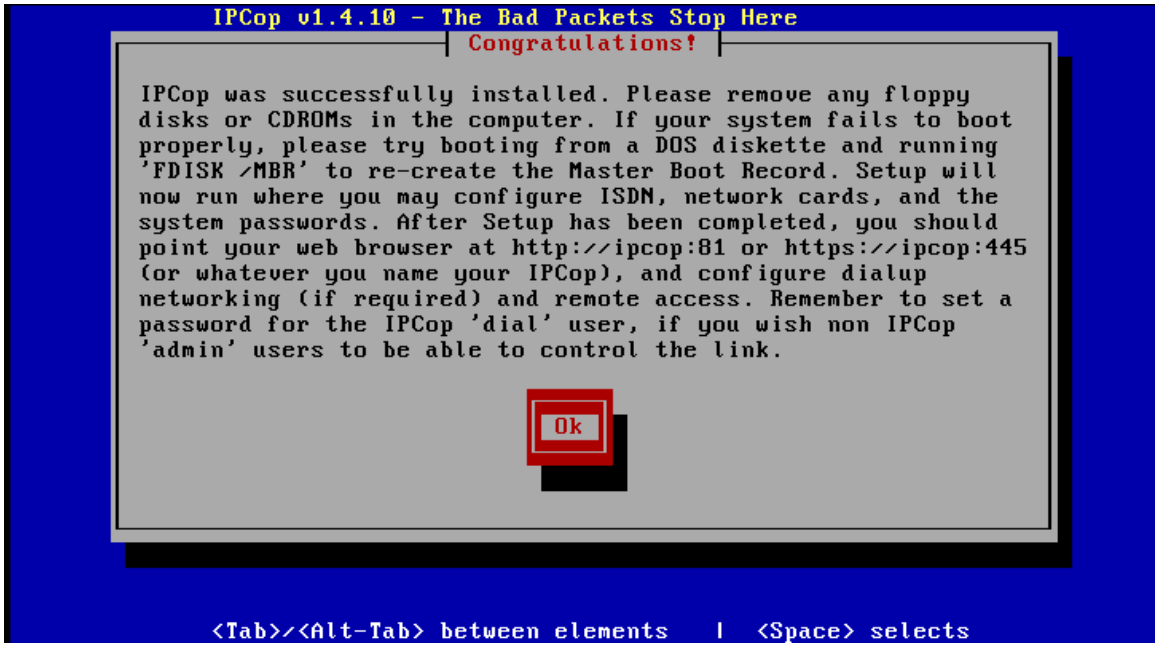
- Next, when you are asked enter your Green Interface an address which must be within your chosen address space (192.168.1.x in our example). Enter in place 192.168.1.1 in the IP address field.



- Following this, IPCop will format and copy itself to your hard drive. See below.



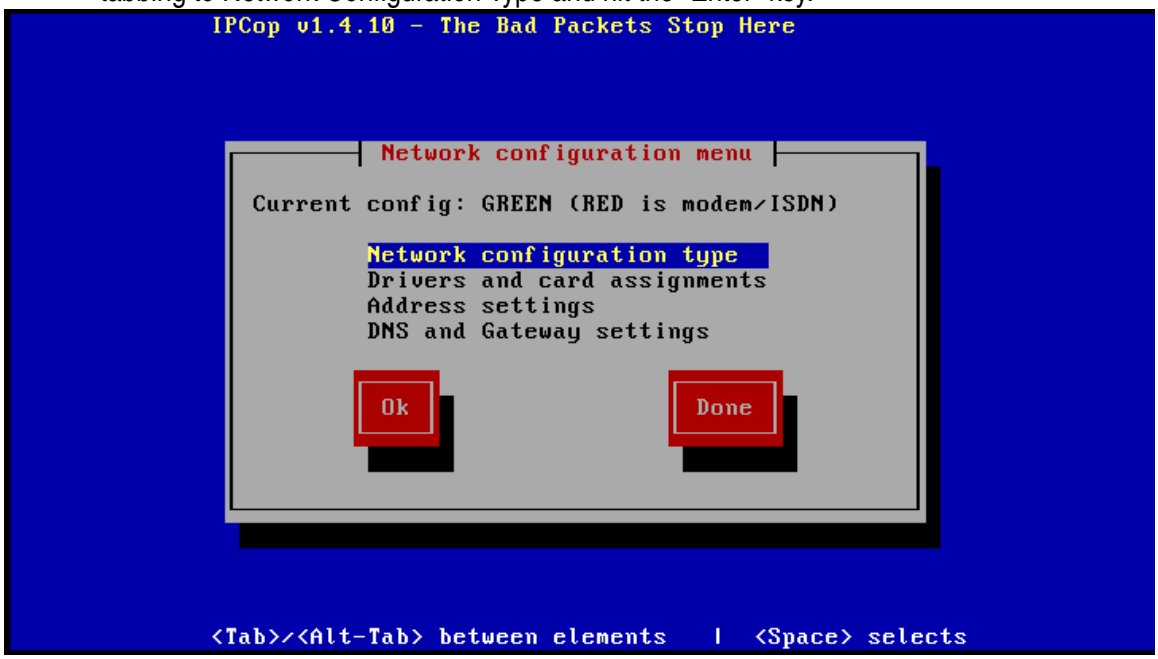
- After the install has completed you will be prompted to reboot and run setup as shown. See below.



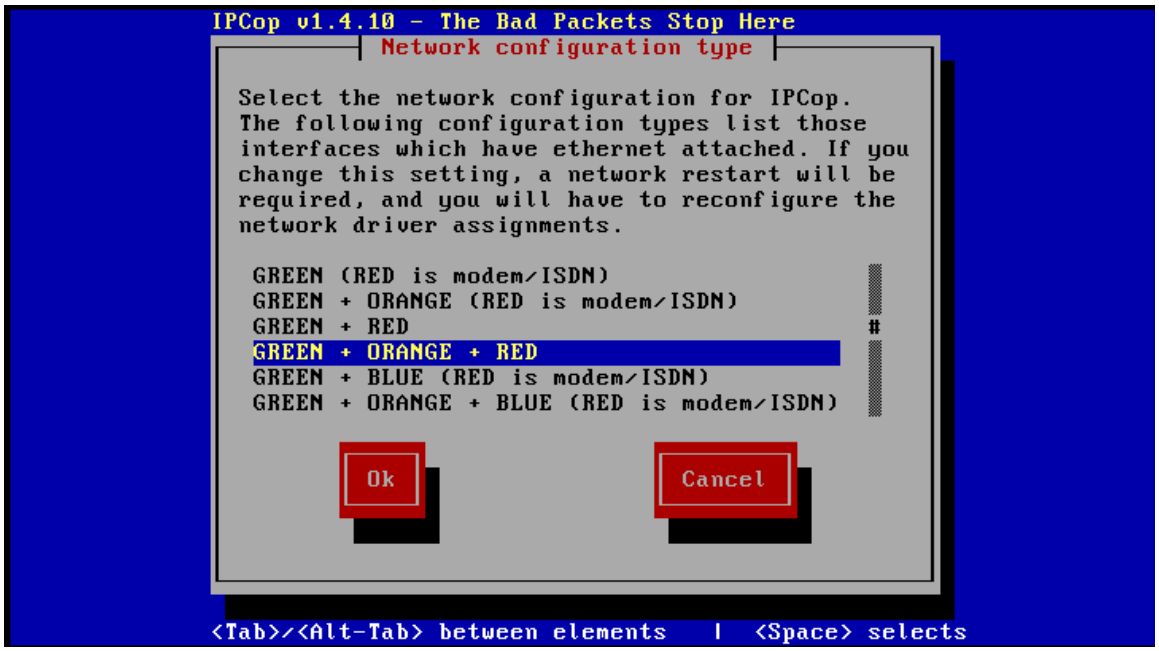
Initial Setup

Having installed IPCop we now have to enter some further configuration information in setup for our setup to be complete.

- Enter in Keyboard, Time Zone and Hostname/Domain.
- ISDN Setup – As you are not using ISDN you should select to ***disable*** it
- Network Configuration Type - Select the Interface configuration you will be running by tabbing to Network Configuration Type and hit the “Enter” key.

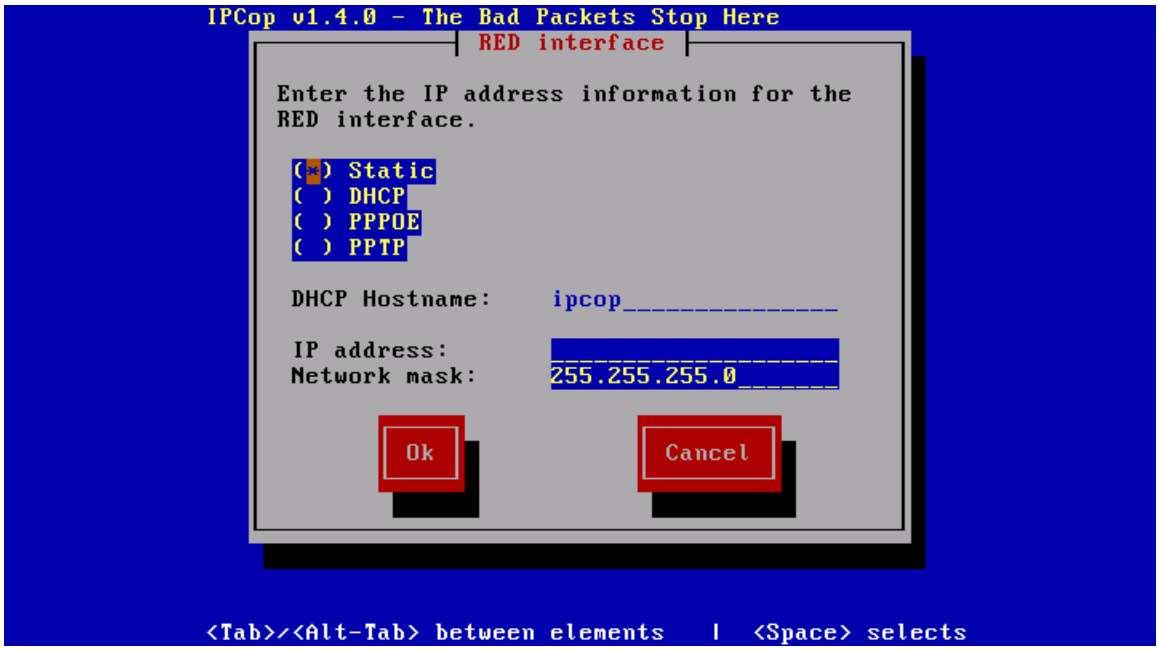


- In our case you would select Red / Orange / Green.



Since we have 3 interfaces and only have set up Green, repeat the interface setup options for the Red and Orange interfaces as described above.

Configure the RED interface to use DHCP as this is interface connected to the Internet (i.e. Your ISP). Then configure your ORANGE interface to use the 192.168.10.x address space. For Red tab over to the DHCP box and select it by hitting Enter. So if your Green network will contain 15 hosts you can use 192.168.1.2-16. To set this up simply add in this range 192.168.1.2-16 and tab down to "OK".



- Password Setup - IPCop has 2 users which you will be asked to setup passwords for the root and admin. Set these both to a strong password > 8 character password that is not a word in any language and contains Caps. A good example would be 1luv19c0p. Root password will be used to log on and add any add-ons or upgrades via SSH. Admin user is used to manage your IPCop day to day.

At the end of the IPCop installation you will be asked to reboot. After reboot go to another machine on your LAN and force your network interface card to update your dynamic (DHCP) address with ifconfig (Linux/Unix) or ipconfig (Windows). Verify you are live and active on the new network you have setup with an address on 192.168.1.x. With this validated connect to secure https web interface of IPCop. Type https://192.168.1.1:445 or https://192.168.1.1:81 and log in as the admin user.

Validate all your settings and connectivity. Then check out all the features you get with this great GNU Open Source Firewall. In the second installment of this how to we will discuss setting up a dynamic DNS, filtering email/web/proxing with Copfilter and allowing access to web/mail server of your choice in the “DMZ” or orange network. Until then Happy Hacking!!

For more info see

IPCop Homepage
http://www.ipcop.org/
IPCop Support
http://www.ipcop.org/1.4.0/en/install/html/
RFC 1918
http://www.ietf.org/rfc/rfc1918.txt
RFC 1631
http://www.ietf.org/rfc/rfc1631.txt